TSC report

Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

2025-08-20T15:27:38 to 2025-08-21T15:27:38

manager.name: wazuh-virtual-machine AND rule.tsc: *

Most common TSC requirements alerts found

Requirement CC8.1

The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives

- Manages Changes Throughout the System Life Cycle
- Authorizes Changes
- Designs and Develops Changes
- Documents Changes
- Tracks System Changes
- Configures Software
- Tests System Changes
- Approves System Changes
- Deploys System Changes
- Identifies and Evaluates System Changes
- Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents
- Creates Baseline Configuration of IT Technology
- Provides for Changes Necessary in Emergency Situations

Top rules for CC8.1 requirement

Rule ID	Description
2904	Dpkg (Debian Package) half configured.
2902	New dpkg (Debian Package) installed.
2901	New dpkg (Debian Package) requested to install.

Requirement CC6.1

Copyright © Codec Networks Pvt Ltd.

The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

- Identifies and Manages the Inventory of Information Assets
- Restricts Logical Access
- Identifies and Authenticates Users
- Considers Network Segmentation
- Manages Points of Access
- Restricts Access to Information Assets
- Manages Identification and Authentication
- Manages Credentials for Infrastructure and Software
- Uses Encryption to Protect Data
- Protects Encryption Keys

Top rules for CC6.1 requirement

Rule ID	Description
550	Integrity checksum changed.

Requirement CC7.2

The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

- Implements Detection Policies, Procedures, and Tools
- Designs Detection Measures
- Implements Filters to Analyze Anomalies
- Monitors Detection Tools for Effective Operation

Top rules for CC7.2 requirement

Rule ID	Description
2904	Dpkg (Debian Package) half configured.
2902	New dpkg (Debian Package) installed.
2901	New dpkg (Debian Package) requested to install.

Copyright © Codec Networks Pvt Ltd.

cnsocservices@codecnetworks.in
https://codecnetworks.com

Requirement CC7.3

The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

- Responds to Security Incidents
- Communicates and Reviews Detected Security Events
- Develops and Implements Procedures to Analyze Security Incidents

Top rules for CC7.3 requirement

Rule ID	Description
2904	Dpkg (Debian Package) half configured.
2902	New dpkg (Debian Package) installed.
2901	New dpkg (Debian Package) requested to install.

Requirement CC6.8

The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

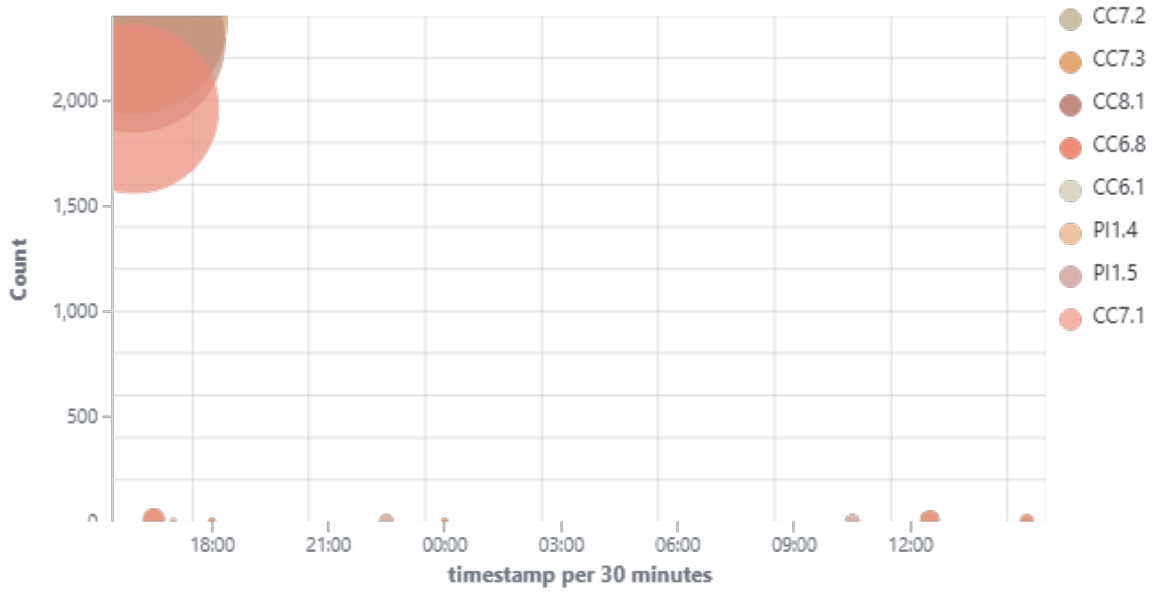
- Restricts Application and Software Installation
- Detects Unauthorized Changes to Software and Configuration Parameters
- Uses a Defined Change Control Process
- Uses Antivirus and Anti-Malware Software
- Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software

Top rules for CC6.8 requirement

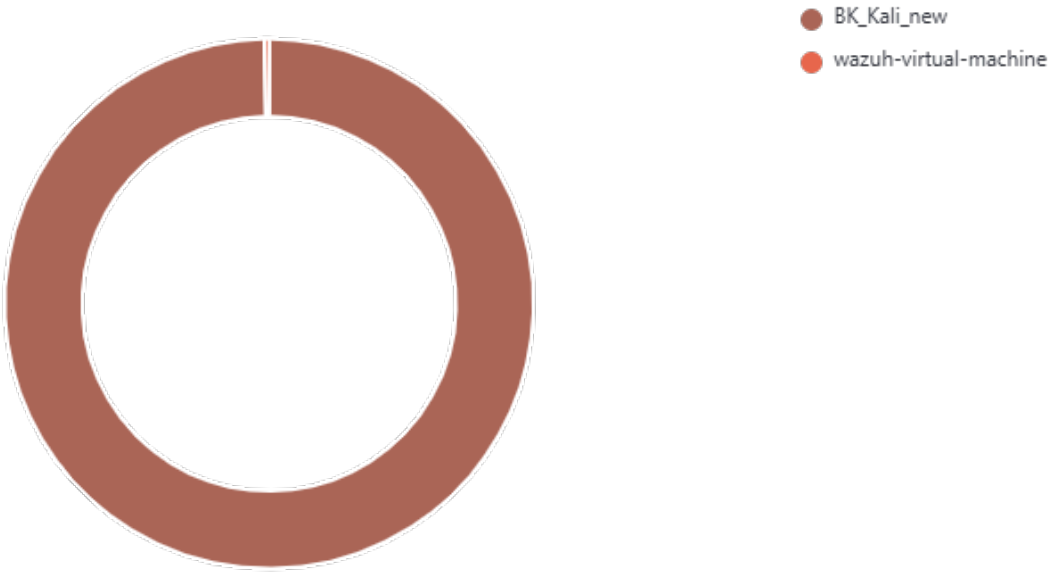
Rule ID	Description
2904	Dpkg (Debian Package) half configured.
2902	New dpkg (Debian Package) installed.
5501	PAM: Login session opened.

Copyright © Codec Networks Pvt Ltd.

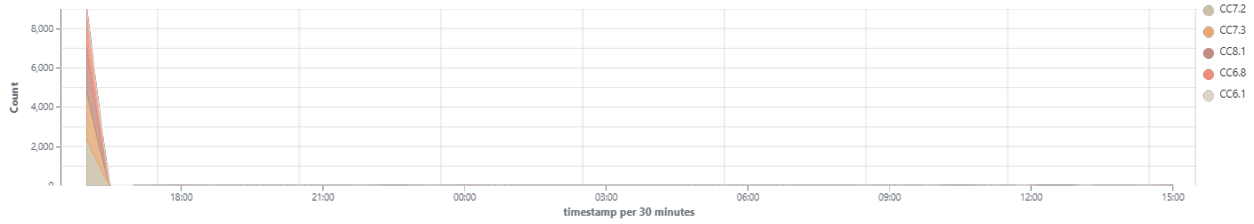
TSC requirements



Top 10 agents by alerts number

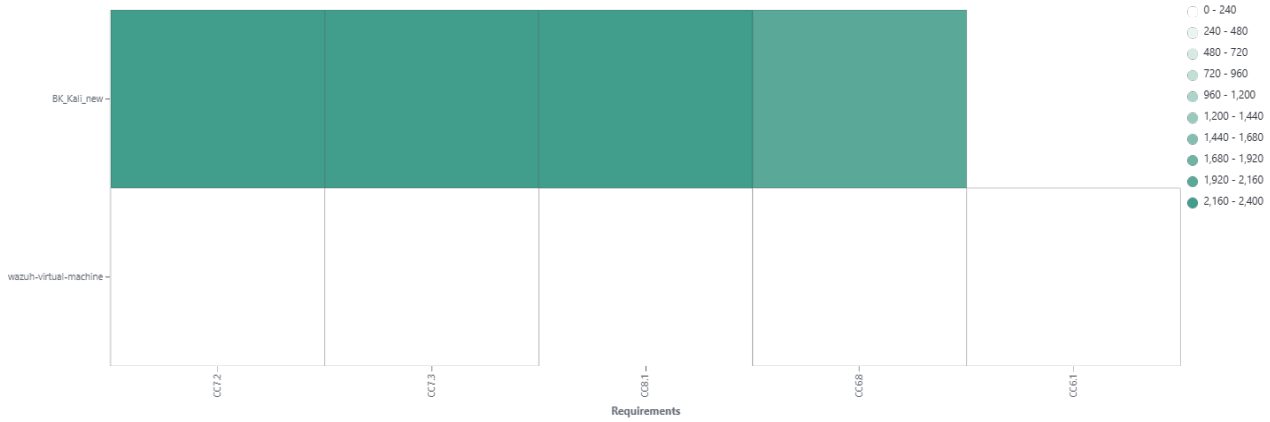


Top requirements over time

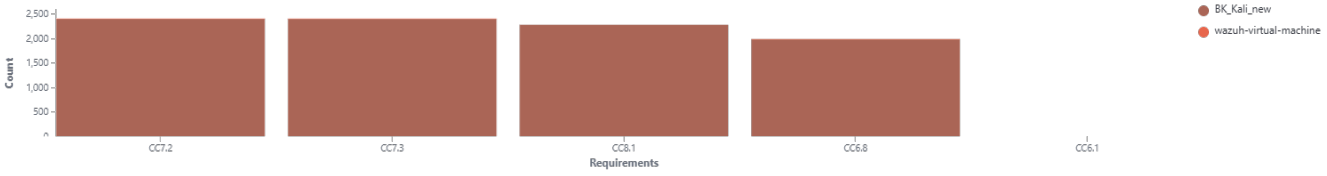


Copyright © Codec Networks Pvt Ltd.

Last alerts



Requirements by agent



Copyright © Codec Networks Pvt Ltd.

Alerts summary

Agent name	Requirement	Description	Count
BK_Kali_new	CC7.2	Dpkg (Debian Package) half configured.	1094
BK_Kali_new	CC7.3	Dpkg (Debian Package) half configured.	1094
BK_Kali_new	CC8.1	Dpkg (Debian Package) half configured.	1094
BK_Kali_new	CC6.8	Dpkg (Debian Package) half configured.	1094
BK_Kali_new	CC7.2	New dpkg (Debian Package) installed.	769
BK_Kali_new	CC7.3	New dpkg (Debian Package) installed.	769
BK_Kali_new	CC8.1	New dpkg (Debian Package) installed.	769
BK_Kali_new	CC6.8	New dpkg (Debian Package) installed.	769
BK_Kali_new	CC7.2	New dpkg (Debian Package) requested to install.	415
BK_Kali_new	CC7.3	New dpkg (Debian Package) requested to install.	415
BK_Kali_new	CC8.1	New dpkg (Debian Package) requested to install.	415
BK_Kali_new	CC7.2	PAM: Login session closed.	38
BK_Kali_new	CC7.2	PAM: Login session opened.	38
BK_Kali_new	CC7.3	PAM: Login session closed.	38
BK_Kali_new	CC7.3	PAM: Login session opened.	38
BK_Kali_new	CC6.8	PAM: Login session closed.	38
BK_Kali_new	CC6.8	PAM: Login session opened.	38
BK_Kali_new	CC7.2	Successful sudo to ROOT executed.	35
BK_Kali_new	CC7.3	Successful sudo to ROOT executed.	35
BK_Kali_new	CC6.8	Successful sudo to ROOT executed.	35
BK_Kali_new	CC7.2	Listened ports status (netstat) changed (new port opened or closed).	4
BK_Kali_new	CC7.3	Listened ports status (netstat) changed (new port opened or closed).	4
BK_Kali_new	CC6.8	Listened ports status (netstat) changed (new port opened or closed).	4
wazuh-virtual-machine	CC6.8	Integrity checksum changed.	4
wazuh-virtual-machine	CC7.2	Integrity checksum changed.	4
wazuh-virtual-machine	CC7.3	Integrity checksum changed.	4
wazuh-virtual-machine	CC6.1	Integrity checksum changed.	4
wazuh-virtual-machine	PI1.4	Integrity checksum changed.	4
wazuh-virtual-machine	PI1.5	Integrity checksum changed.	4
BK_Kali_new	CC7.2	Wazuh agent started.	2
BK_Kali_new	CC7.3	Wazuh agent started.	2
BK_Kali_new	CC6.8	Wazuh agent started.	2
wazuh-virtual-machine	CC6.8	PAM: Login session opened.	2
wazuh-virtual-machine	CC7.2	PAM: Login session opened.	2
wazuh-virtual-machine	CC7.3	PAM: Login session opened.	2
BK_Kali_new	CC7.2	Dpkg (Debian Package) removed.	1
BK_Kali_new	CC7.2	The CVE-2025-47278 that affected Flask was solved due to an update in the agent or feed.	1
BK_Kali_new	CC7.2	Wazuh agent disconnected.	1
BK_Kali_new	CC7.2	Wazuh agent stopped.	1

Copyright © Codec Networks Pvt Ltd.

Agent name	Requirement	Description	Count
BK_Kali_new	CC7.3	Dpkg (Debian Package) removed.	1
BK_Kali_new	CC7.3	Wazuh agent disconnected.	1
BK_Kali_new	CC7.3	Wazuh agent stopped.	1
BK_Kali_new	CC8.1	Dpkg (Debian Package) removed.	1
BK_Kali_new	CC6.8	Dpkg (Debian Package) removed.	1
BK_Kali_new	CC6.8	Wazuh agent disconnected.	1
BK_Kali_new	CC6.8	Wazuh agent stopped.	1
BK_Kali_new	CC7.1	The CVE-2025-47278 that affected Flask was solved due to an update in the agent or feed.	1
wazuh-virtual-machine	CC6.8	Listened ports status (netstat) changed (new port opened or closed).	1
wazuh-virtual-machine	CC7.2	Listened ports status (netstat) changed (new port opened or closed).	1
wazuh-virtual-machine	CC7.3	Listened ports status (netstat) changed (new port opened or closed).	1

Copyright © Codec Networks Pvt Ltd.